CREDIT CARD MERCHANT PROCEDURES MANUAL

Effective Date: 04/29/2016

Updated: April 29, 2016

TABLE OF CONTENTS

INTRODUCTION

The University of Central Florida accepts credit card payments as a convenience to its customers. University merchants may accept VISA, MasterCard, Discover, American Express, Diner's Club and debit cards with a VISA or MasterCard logo per the terms of the university's merchant services provider contract.

A university merchant is any University of Central Florida business unit that accepts credit/debit cards as a form of legal tender, including retail and Web-based operations. University merchants are responsible for compliance by their third-party service providers who accept debit/credit payments that deposit to the university's bank account. See further discussion concerning third-party vendors in the following section.

Compliance with this manual is required by UCF policy 3-206.5, "Credit Card Merchant Policy", which applies to any employee, contractor, agent, or service provider who stores, processes, or transmits cardholder data on behalf of university merchants accepting credit and/or debit cards. This policy applies to all credit/debit card transactions.

Each university merchant's Dean, Director or Chair or their appropriate designee is responsible for compliance with this policy and the related procedures within this manual. The person assigned as the appropriate designee must have the sufficient level of management authority within the department. "DDC" referenced throughout this document includes the DDC's designee as defined herein.

The procedures outlined herein are designed to protect cardholder data; maximize the university's compliance with its merchant services provider contract, which includes compliance with the Payment Card Industry's Data Security Standards (PCI DSS) and the various credit card brand standards; and to ensure appropriate integration with the university's financial and other systems.

THIRD-PARTY VENDORS

Third-party vendors are classified into two categories for the purposes of this manual. The first category refers to third-party vendors that contract to do business with and accept credit/debit payments on behalf of a university merchant. The payments accepted by these third-party vendors must deposit to the university's bank account. Examples of this type of third-party vendor include the registration systems within the First Year Experience department or reserved seating systems within the UCF Theatre. These third-party systems are used to meet the specific business needs of certain university merchants when they cannot be provided by our current bank contract. Additionally, a third party vendor may be selected for one time/low volume merchant needs. Guidelines governing this type of third-party vendor are contained within this manual.

The second category of third-party vendors refer to vendors who contract to do business as a location on UCF property. Examples of this type of third-party vendor include the food locations at the student union or the arena, the university bookstore provider (Barnes & Noble) and the university cafeteria meal plans (Aramark). While these vendors are outside the scope of this policy, it is imperative the initiating department ensures these third-party contracts with the

university address compliance with PCI DSS. Security breaches arising from any non-compliance issues could result in damage to the university's reputation.

MERCHANT ACCOUNT SET-UP

A merchant account is required in order to accept receipts from credit/debit card transactions. All merchant accounts are created through the university's merchant services provider contract. University merchants must abide by the terms of this contract as well as with university policies contained within this manual.

To establish a merchant account, **or make changes to an existing merchant account**, the first step is to contact the Merchant Services Accounting Coordinator (MSAC) in UCF's Finance and Accounting Department (contact information is presented at the end of this manual). The Merchant Services Committee (MSC) facilitates the review and approval process. Approval from the University Controller is required to establish a merchant account.

The MSC will meet with the business unit to assist in the determination of its needs, including but not limited to hardware, software, system requirements, business practices, accounting support, financial reporting, tax implications and reporting requirements.

The MSC will determine if the business unit requires the setup of a new auxiliary department. If an auxiliary department needs to be created, the business unit must complete Form 41-656 *Request to Operate an Education Business Activity* and return it to Finance and Accounting.

After the merchant account is approved the following steps take place:

1) Applications. Various applications are necessary to obtain merchant account numbers from the credit card brands. First, an application is sent to American Express. Once the American Express account number has been provided, then an application is sent to the university's merchant services provider to obtain VISA, MasterCard and Discover account numbers. The university merchant services bank will provide the business unit with its own merchant account, a sub-account of the overall university's main merchant account.

2) Selection of a third-party vendor. Third-party vendors process credit card transactions securely from outside the university environment, relieving the university's liability of maintaining and storing credit card data, provided all other internal security measures are taken (see the Compliance section). All third-party vendors must be approved by the MSC and meet the following requirements:

    a. Compliant with the *Payment Card Industry Data Security Standards* (see Compliance section).

    b. Adhere to the university's merchant services provider contract.

    c. Does not store credit card data.

d. Be an approved processor per the merchant service provider's list of approved processors.

3) Testing. Before credit card payments can be accepted, testing of the applications and systems must occur. The testing takes place first in a demo environment and then in a live environment and verifies transactions, including voids and credits, post to the university's general ledger and bank properly. *Note: These tests must be re-performed when any notable changes occur, such as server changes, computer systems or application upgrades*.

4) Personnel. The roles and responsibilities of the business unit's personnel will determine what training, certification and or other requirements, such as background checks need to be completed prior to handling credit card data. See the Personnel Requirements section.

5) Self-Assessment Questionnaire (SAQ). The PCI DSS SAQ must be completed annually, each March/April and assistance should be provided by the department's IT personnel in collaboration with the MSC. See the SAQ section below.

The MSC acts as the liaison between the business unit and various outside vendors, including third-party vendors, to provide support throughout the merchant account set-up, integration, and implementation processes. The amount of time required to set-up and activate a merchant account varies based on the nature of the business unit's environment, processes, and the extent of involvement by external contractors or consultants.

PERSONNEL REQUIREMENTS

Prior to receiving access to cardholder data, merchant employees, contractors and agents must:

1) Have a background check by UCF Human Resources. Employees with an inappropriate background, as determined by MSC, may not be permitted to have access to cardholder information. Each instance will be reviewed on a case-by-case basis. *Exception: UCF Finance and Accounting makes exceptions on an individual basis for students taking specific UCF courses or receiving grants requiring them to perform duties where credit card information is handled as part of their course requirements. These students may be exempt from having a background check. Students are governed by UCF's Code of Conduct contained within the UCF Golden Rule Student Handbook.*

   Merchants must pay for a background check for any volunteers or OPS staff member employed less than a year. Otherwise, UCF's Human Resources department will routinely perform the background check at the time the staff member has been employed for one year, with no charge to the merchant.

2) Successfully complete the online "FSC111: Credit Card Information Security" training session or a security awareness program offered by UCF. See the link in the Resources section below.

3) Sign the "Credit Card Security Ethics Certification" (Form 41-915) to document his or

her understanding of and willingness to comply with all university credit card policies and procedures. This certification will be maintained by F&A. See the link in the Resources section below.

Annually, merchant employees, contractors or agents are required to do the following:

1) Successfully complete the online "FSC111: Credit Card Information Security" training session.

2) Provide written certification by their DDC or the DDC's designee that such training has occurred for all merchant employees and has been documented by signing the UCF Merchant Services compliance certification form after their respective self-assessment questionnaire (SAQ) has been completed.

ACCOUNTING FOR DEPOSITS AND RECONCILIATIONS

Reconciliations are necessary to ensure transactions are accounted for properly and posted to the correct university department. The following reconciliations should be performed by each university merchant on a daily basis:

1) Compare the merchant's internally generated transaction report to the third-party processor's settlement statement to ensure both the number and the total amount of transactions generated at the merchant location is consistent with the transactions settled by the third-party processor. Once this reconciliation is completed, the merchant provides this settlement statement to the university cashier's office for posting to the university general ledger.

2) After the cashier's office has posted the deposits to the general ledger, compare the merchant departmental revenue amount in the university general ledger to the deposit amount on the third-party processor's settlement statement to ensure deposits were posted to the correct department.

Any discrepancies between the internally generated transaction statement and the third-party processor's settlement statement must be researched by the university merchant with their third-party processor. Please contact the MSAC for assistance with performing these reconciliations or resolving discrepancies.

MERCHANT FEES

Various fees are incurred by university merchants for accepting credit cards payments. These fees are charged to each university merchant's department determined at merchant set-up. The fees are based on the monthly detailed statements provided by the third-party processor, the credit card companies and the university bank. These fees include:

- **Interchange fees**. Fees charged by the purchaser's credit card issuing bank.

- **Assessment fees**. Fees charged by the purchaser's credit card brand (i.e. VISA, MasterCard, Discover, American Express, etc.).

- **Merchant Account Provider fees**. Fees charged by the university's merchant services account provider.

- **Transaction fees**. Fees charged to the university by the university merchant's third-party processors.

CONVENIENCE FEES

Approval is required from the University Controller to allow university merchants to charge convenience fees to their customers so they may use an alternative payment channel. Currently, these fees are allowed to be charged only for Internet sales as long as the merchant provides customers with another option to make payments where no convenience fee is charged.

The following conditions must be met:

1) The fee is charged with the total purchase.

2) A flat fee or a percentage of the total purchase may be assessed.

3) The convenience fee charged may not exceed the total fees incurred by the merchant.

University merchants must be aware that the rules regarding convenience fees are ever-changing and determined by the various credit card brands.

COMPLIANCE

Security breaches can result in serious consequences for the university, and may include release of confidential information, damage to reputation, added compliance costs, the assessment of substantial fines, and possible legal liabilities. The DDC, or their designee of each university merchant is required to ensure that appropriate controls are implemented and monitored to ensure compliance with this manual and the security standards discussed below.

All university business units that handle, store, process, or transmit cardholder data, including any UCF employee, contractor or agent who, in the course of doing business on behalf of the University, is involved in the acceptance of credit cards and E-commerce payments for the University, must comply with the Payment Card Industry's Data Security Standards (PCI DSS).

The PCI DSS's are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The Council is responsible for managing the security standards, while compliance is enforced by the payment card brands. These standards include controls for handling and restricting credit card information, computer and internet security, as well as the reporting of a credit card information breach.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI DSS)

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processed.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security.

For more details, consult https://www.pcisecuritystandards.org

TOOLS FOR ASSESSING COMPLIANCE WITH PCI DSS

The PCI SSC sets the PCI DSS standards, but each card brand has its own program for compliance validation levels and enforcement. University merchants should be familiar with all of the individual credit card brand standards and refer to them periodically. These standards contain not only security standards but transactional standards which are *not* included in compliance procedures table in the Appendix. More information about compliance with specific credit card brands can be found at these links.

- American Express: www.americanexpress.com/datasecurity
- Discover Financial Services: http://www.discovernetwork.com/merchants/data-security/disc.html
- MasterCard Worldwide: http://www.mastercard.com/sdp
- Visa Inc.: http://usa.visa.com/merchants/operations/op_regulations.html

COMPLIANCE PROCEDURES

University merchants must comply with various security standards including the Payment Card Industry's Data Security Standards; the various credit card brands security standards; and the university security standards referenced in the university's policies contained within this manual. Refer to the above section for further guidance. To facilitate compliance with all of these standards, review the compliance procedures table in the Appendix which outlines specific

procedures by the accountable party, including personnel, merchant, University Finance and Accounting, and University Computer Services & Telecommunications departments. Note that the various credit card brands transactional standards are not included in the compliance procedures table; refer to the above section for further guidance.

SELF-ASSESSMENT QUESTIONNAIRE (SAQ)

To comply with PCI DSS standards, all university merchants must complete the annual SAQ each September and in the event of any major change to an application or server.

The university merchants complete their SAQ using an external provider, *Coalfire* which is a certified remote-assessment and compliance solution designed to help merchants meet the security standards of all credit card companies. With the assistance of the MSAC, the university merchants enroll in *Coalfire's* program (located in Resources below). The university merchant completes the electronic SAQ *in Coalfire's* program. Once the SAQ is completed a merchant will receive a percentage of completion and must continually answer the questions, making corrections as needed until a 100% score is received. Merchants who obtain a 100% score are considered PCI compliant and receive an "Attestation of Compliance" report. Merchants are encouraged to obtain assistance from the MSC in order to obtain successful completion of the SAQ. The university MSAC monitors the university's various Coalfire SAQ accounts to ensure timely and successful completion.

University merchants may use the evidence tab within the Coalfire system to store external vendor compliance documentation, such as the vendor's PCI compliance certificate. Also, contracts with external vendors should be stored in this digital locker. This includes external vendors who provide system/application repair and maintenance, IT support, etc.

University merchants are permitted and encouraged to print out their SAQ's "Attestation of Compliance" reports, and display at their merchant locations, either physically or in digital format for online activity.

The university merchant department's DDC, or their designee, must attest to the completion of this SAQ annually by signing the *UCF Merchant Services Compliance Certification* form.

NETWORK SCANS

PCI DSS requires both internal and external network vulnerability scans be performed at least quarterly and after any significant change in the network (such as new system component installations, firewall modifications, product upgrades). The university merchants and UCF CS&T share this responsibility.

UCF CS&T runs the *external* vulnerability scans on all Web application servers, including the university merchant's Web application servers accessible from the internet, monthly. The results of the scans are sent to the merchant's IT/security contacts monthly for review.

University merchants should be scanning their *internal* networks (such as all of their work stations, local file servers, etc.), at least quarterly and after any significant change in their

network (such as new system component installations, firewall modifications, product upgrades). CS&T provides the tools to the university merchant's IT/security contact to perform these scans per the university merchant's request for assistance from CS&T.

The university merchant department's DDC or their designee, must attest to the completion of these scans annually by signing the *UCF Merchant Services Compliance Certification* form.

PENETRATION TESTING

PCI DSS requires penetration testing be performed both inside and outside the network at least annually and after any significant change in the network (such as new system component installations, firewall modifications, product upgrades).

UCF CS&T will work with a vendor to perform the penetration testing and collaborate with university merchants to correct vulnerabilities.

The university merchant department's DDC or their designee, must attest to the completion of these scans annually by signing the *UCF Merchant Services Compliance Certification* form.

RESPONDING TO A SECURITY BREACH

In the event of a breach or suspected breach of security, including the suspicion that credit card information has been exposed, stolen, or misused, the university merchant must immediately contact the following departments.

- UCF Computer Services & Telecommunications, University Information Security Officer, Service Desk, 407-823-5117 sirt@ucf.edu
- UCF Finance & Accounting, Merchant Services Coordinator, 407-882-1000 famerchsup@ucf.edu

Immediately contain and limit the exposure to preserve evidence and facilitate the investigation by doing the following:

- Do not access or alter compromised systems.
- Do not turn compromised systems off.
- Preserve logs and electronic evidence.
- Document all actions taken.
- Be on "high" alert and monitor all systems with cardholder data.

Refer to the UCF Computer Services and Telecommunications Web site for further instructions and forms.

ENFORCEMENT

University merchants not in compliance with UCF policy 3-206.5, "Credit Card Merchant Policy" will be suspended from processing services.

POLICY AND PROCEDURE MANAGEMENT

The university may modify these directives and procedures from time to time as required, provided that all modifications are consistent with PCI Data Security Standards currently in effect. The MSC is responsible for initiating and overseeing a review of the "UCF Credit Card Merchant Policy" and the corresponding "UCF Credit Card Merchant Procedures Manual", making appropriate revisions and updates and disseminating the revised directives and procedures to university merchants. Updates to procedures will be made on a timely basis to coincide with the three year cycle of updates to the PCI DSS.

CONTACTS

UCF Finance and Accounting, Merchant Services
Merchant Services Accounting Coordinator, Ann Boutros
407-882-1040
Ann.Boutros@ucf.edu
famerchsup@ucf.edu

UCF Computer Services & Telecommunications
Information Security Officer, Chris Vakhordjian
407-823-3863
chrisv@ucf.edu
infosec@ucf.edu
sirt@ucf.edu

RESOURCES

UCF Finance and Accounting, Merchant Services Web Site

"Credit Card Information Security Training" (FSC 111)

Form 41-656, "Request to Operate an Education Business Activity"

Form 41-915, "Credit Card Security Ethics Certification"

Payment Card Industry Security Standards Council Data Security Standards

UCF Computer Security Standards and Guidelines

Coalfire's SAQ Program login

University Security Incident Response Plan

APPENDIX: COMPLIANCE PROCEDURES TABLE

Compliance Procedures	Prior to cardholder data access	Continuously	Quarterly	Annually
Employees / Contractors / Agents with access to credit card data must:				
Have an acceptable background check by UCF Human Resources	**X**			
Complete the *Credit Card Data Security, FSC 111* training provided on-line by UCF Finance and Accounting (see link in Resource section)	**X**			**X**
Sign the Form 41-915 *Credit Card Security Ethics Certification* (see link in the Resource section) to document the understanding of and willingness to comply with all university credit card security policies, directives and procedures	**X**			
University Merchants must:				
Ensure the PC(s) used to connect to a payment gateway - Comply with the computer security standards outlined at www.infosec.ucf.edu. - Blocks outside internet access except to the Payment Gateway. - Prohibits the use of e-mail to avoid security breaches. - Security level zone set to "high" for the Internet. - Require each user to have unique sign-on identification.		**X**		
Develop and document a set of *Standard Operating Procedures*. At a minimum, these procedures should cover how specific types of transactions are handled; specific requirements necessary to comply with the university's procedures outlined within this manual; the rights of each type of employee (for example, cashier vs. merchant administrator); and the process for responding to a security breach per the university security incident response plan (see link below in the Resource section. These procedures		**X**		**X**

Compliance Procedures	Prior to cardholder data access	Continuously	Quarterly	Annually
should be updated annually.				
Be familiar with the individual payment card brand requirements. (See Tools for Assessing Compliance with PCI DSS section above).		**X**		
Appoint a security coordinator/contact and one or more back-up contacts. Coordinators/Contacts need to have familiarity with business operations and computer systems in their departments. It is not necessary for the contact to have extensive security expertise.		**X**		
Communicate any infrastructure, system or process changes to the MSAC.		**X**		
Limit and secure access to system components and cardholder data to only those individuals whose job requires such access.		**X**		
Assign a unique ID to each person with computer access.	**X**			
Provide each user with a unique password that expires after ninety days to access credit card data.		**X**		
Protect cardholder information so that no more than the first six and the last four digits of the credit card number are displayed or printed.		**X**		
Cardholder information should not be stored unless it is critical to on-going business transactions. If storing cardholder information is necessary, then storage of this information must be reported on the annual self-assessment questionnaire; and with knowledge of the university Information Security Officer. Any cardholder information stored should be secured with access limited to only those individuals whose job requires such access. Store only cardholder data that is encrypted or truncated. The three or four digit validation code (CVV) should *never* be stored.		**X**		
Not release credit card information in any form unless there is a legitimate business purpose and then only after the request for information has been reviewed and approved by university merchant management.		**X**		
Not store cardholder information on desktops, laptops, notebooks, or mobile computing devices at any time.		**X**		

Compliance Procedures	Prior to cardholder data access	Continuously	Quarterly	Annually
Prohibit transmitting credit card information by e-mail or fax		**X**		
Store and secure cardholder data in locked containers identified and classified as confidential in secured areas with limited access. Examples include electronic data, customer receipts, merchant duplicate receipts, and reports.		**X**		
Cardholder data must be disposed of by overwriting or degaussing magnetic media or cross-shredding paper.			**X**	
Review your off-site storage facilities to ensure all security requirements are met.				**X**
Provide secure access of the cardholder data at all times if wireless connections are used, and test controls, limitations, network connections, and restrictions to stop unauthorized access attempts. A wireless analyzer must be used at least quarterly to identify all wireless devices in use for their compliance with Payment Card Industry (PCI) Data Security Standards (DSS).Any wireless activity must be approved by the University Information Security Officer.				**X**
Maintain inventory logs of all media and conduct media inventories at least annually				**X**
Review access logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol servers.		**X**		
Retain audit trail history (i.e. logs) for all system components for at least one year, with a minimum of three months immediately available for analysis (ex: online, archived, or restorable from back-up).		**X**		
Deploy anti-virus software on all systems commonly affected by viruses and ensure that the programs are capable of detecting, removing, and protecting from other forms of malicious software, including spyware and adware.		**X**		
Educate staff at least annually on UCF's credit card policy and procedures to build awareness of the importance of cardholder data security. Staff acknowledgement of this education needs to be documented with signatures of the staff attesting to this communication.				**X**

Compliance Procedures	Prior to cardholder data access	Continuously	Quarterly	Annually
Run internal network vulnerability scans using UCF Computer Services & Telecommunication (UCF CS&T) provided tools at least quarterly and after any significant change on their network (such as new system component installations, product upgrades, etc.). Merchants should make a formal request with CS&T to get assistance with this process.			**X**	
Perform a self-assessment using the PCI Security Council's self-assessment questionnaire (SAQ), annually, in the month of March/April; correct all identified weaknesses as soon as possible but no later than 90 days after weaknesses are identified, or face suspension.				**X**
Test the incident response plan annually				**X**
Use the university's merchant services provider for all credit card processing.		**X**		
With respect to university merchant third-party vendors, merchants must:				
Provide all third-party vendors with a copy of university credit card policies.	**X**			
Provide all third-party vendors with a unique user ID that includes a password that expires every sixty days via the UCF's Information Security Office's *UCF Account/Access/Termination Request Form.* This ID is only provided upon need. (See link to form in the Resources section below).	**X**	**X**		
Give third-party vendors access to credit card data only after a formal contract is signed that outlines the security requirements and requires adherence to the payment card industry security requirements. This contract should be kept in each merchant's Evidence tab in *Coalfire's program* along with the vendor's PCI compliance certificate (See Self-Assessment Questionnaire section below).	**X**			**X**
Maintain a list of all third-party vendors and provide this list and contracts with providers to Finance and Accounting, Merchant Services.		**X**		
Maintain a program to monitor service providers' PCI Standards compliance status at least annually, and maintain documentation to support their compliance.				**X**
UCF Finance & Accounting must:				

Compliance Procedures	Prior to cardholder data access	Continuously	Quarterly	Annually
Establish, review, and disseminate a security policy along with procedures that address all security requirements with updates provided to incorporate changes to business objectives or the risk environment (i.e. "Credit Card Merchant Policy" and "Credit Card Merchant Procedures Manual").		**X**		
Administer merchant accounts, including additions, deletions, and modifications. Coordinate the annual PCI self-assessment questionnaire in partnership with an independent compliance partner that is certified by the cardholder industry (see Self-Assessment Questionnaire section below)		**X**		
Develop, maintain and provide the "Credit Card Information Security Training" and the "Credit Card Security and Ethics Certification".		**X**		
Monitor university merchant locations annual PCI Security Council's self-assessment questionnaires for compliance and suspend non-compliant merchant accounts when identified weaknesses are not corrected in a reasonable period of time.				**X**
UCF Computer Services and Telecommunications (UCF CS&T) must:				
Actively work with university merchant location staff to ensure the security of their technical environment meets the requirements set forth by university standards.		**X**		
Establish, document, publish, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations (i.e. contained within the "Credit Card Merchant Policy" and "Credit Card Merchant Procedures Manual").		**X**		
Monitor and analyze security alerts and information, and distribute to the appropriate merchant contacts.		**X**		
Establish firewall and router configuration standards with review of firewall and router rule sets every six months.			**X**	
Perform penetration testing at least once a year and after any significant infrastructure upgrade or when a sub-network or Web server is added to the environment.				**X**

Compliance Procedures	Prior to cardholder data access	Continuously	Quarterly	Annually
Run vulnerability scans on internet facing systems, such as publicly facing Web applications at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall modifications, product upgrades).			**X**	
Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files and perform critical file comparisons daily.		**X**		
Review access logs daily for all system components.		**X**		
Maintain audit trail history in hard copy for at least one year and for at least three months online.			**X**	**X**